UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/693,149	10/23/2003	Frederick S. M. Herz		1678

23377 7590 12/11/2007
WOODCOCK WASHBURN LLP
CIRA CENTRE, 12TH FLOOR
2929 ARCH STREET
PHILADELPHIA, PA 19104-2891

EXAMINER	
WYSZYNSKI, AUBREY H	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
12/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/693,149	**Applicant(s)** HERZ, FREDERICK S. M.	
	Examiner Aubrey H. Wyszynski	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 September 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-21* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 September 2007* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

1. The response of 9/17/07 was received and considered.

2. Claim 1 is canceled. Claims 2-21 are newly added.

Response to Arguments

3. Applicant's amendment, filed 9/17/97, has canceled claim 1 and claims 2-21 are newly added. Therefore, a new ground of rejection is necessitated.

4. Applicant's arguments with respect to claims 2-21 have been considered but are moot in view of the new ground(s) of rejection.

Specification

5. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: Distributed computer network security activity model SDI-SCAM.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 2-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Rowland, US Patent 6,405,318.

Regarding claim 2, Rowland discloses a system that detects the state of a computer network, comprising: at least one agent/host local controller (fig. 9, #151-153) disposed in said computer network, each said agent/host local controller, comprising:
data collection means/intrusion detection system (fig. 1) for passively collecting, monitoring, and aggregating data representative of activities of respective nodes within said computer network (log file auditing, fig. 2, and col. 2 lines 40-47);
means responsive to the data from the data collection means for analyzing said data to develop activity models/user profile data or signatures, representative of activities of said network in a normal state and activities of said network in an abnormal state; and
means for comparing collected data to said activity models to determine the state of said computer network at different times and to dynamically update said activity models (col. 2 . lines 40-67 and fig. 2).

Regarding claim 3, Rowland discloses the system of claim 2, wherein said at least one agent comprises a plurality of distributed agents/host local controllers and central system controller (fig. 9. #150 and #151-153).

Regarding claim 4, Rowland discloses the system of claim 2, wherein said data collection means collects data representative of operation of said computer network, including respective nodes in said computer network, said data relating to communications, internal and external accesses, code execution functions, and/or network resource conditions of respective nodes in said computer network (col. 2 lines 40-67, Rowland discloses the system coordinates information transfer with host, multi-host and network environments to coordinate intrusion response...real-time monitoring of log audit files, port scan detection and session monitoring. Fig. 3 demonstrates monitoring foreign domains).

Regarding claim 5, Rowland discloses the system of claim 2, wherein said activity models characterize conditions within said computer network including behaviors, events, and/or functions of respective nodes of said computer network, said behaviors representative of said normal state and one or more abnormal states representative of suspicious activity in said computer network. (col. 2 lines 40-67 disclose the intrusion detection system automatically and dynamically builds user profile data for each user that can be used to determine normal actions for each user to reduce the occurrence of false alarms... and fig. 2 shows monitoring suspicious events #15, known attacks, #12, known security violations, #13).

Regarding claim 6, Rowland discloses the system of claim 2, further comprising means for characterizing the state of the computer network and identifying any potential threats based on said collected data (figs 4-5 disclose the user profile database and user database update function and the anomaly detection function).

Regarding claim 7, Rowland discloses the system of claim 6, wherein said characterizing means further recommends remedial repair and/or recovery strategies to isolate and/or neutralize the identified potential threats to the computer system (in the event of a detected threat the control is notified, fig. 5, #55, fig. 6, #85, fig. 7, #97; in fig. 8, determine and take appropriate action #127-136).

Regarding claim 8, Rowland discloses the system of claim 2, wherein respective agents are connected by redundant communications connections (fig. 9).

Regarding claim 9, Rowland discloses the system of claim 2, wherein each agent is implemented in redundant memory and hardware that is adapted to be insulated from infected components of said computer network (col. 2, lines 48-67).

Regarding claim 10, Rowland discloses the system of claim 2, wherein the agents a plurality of agents are disposed in a hierarchical structure whereby communications from bottom level agents to agents at higher levels in the hierarchy are limited (fig. 9, local host controller, central system controller, network administrator).

Regarding claim 11, Rowland discloses the system of claim 2, further comprising means for predictively modeling the behavior of said computer network based on sequentially occurring behavior patterns in the data collected by said data collection means (col. 5, lines 30-35 and figs. 3-4).

Regarding claim 12, Rowland discloses the system of claim 2, wherein said comparing means comprises means for pattern matching collected data with data in said activity models to determine a closest activity model based upon similarity of the data in each data model with the collected data (col. 5, lines 30-35 and figs. 3-4).

Regarding claim 13, Rowland discloses the system of claim 2, wherein the collected data represents actions of a virus, system responses to actions of a virus, actions of a hacker, system responses to actions of a hacker, threats directed to discrete objects in said computer network, and/or potential triggers of a virus or threat to said computer network (col. 6, lines 13-col. 7, line 40 and fig. 6).

Regarding claim 14, Rowland discloses the system of claim 2, wherein said analyzing means for each agent filters and analyzes received data and dynamically redistributes the analyzed and filtered data to other agents associated with said each agent (col. 2, lines 50-66).

Regarding claim 15, Rowland discloses the system of claim 2, wherein said analyzing means performs a pattern analysis on the collected data and said comparing means compares the results of the pattern analysis to the results of pattern matching by analyzing means of other agents to identify similar patterns of suspicious activity in different portions of the computer network (col. 2, lines 50-66 and col. 5, lines 30-35 and figs. 3-4).

Regarding claim 16, Rowland discloses the system of claim 2, wherein the comparing means compares names and email addresses in said collected data against known criminal, hoaxsters and/or aliases for known criminals and hoaxsters (col. 10, 27-35 and col. 6, lines 30-51, SMTP).

Regarding claim 17, Rowland discloses the system of claim 2, further comprising a trusted server that receives attack data from a plurality of agents identifying abnormal states indicative of a network attack, said trusted server gathering the attack data and sending warnings to selected nodes in said computer network (fig. 9, #150, central system controller).

As per claim 18, this is a method version of the claimed system discussed above in claim 1 wherein all claimed limitations have also been addressed and/or cited as set forth above.

Regarding claim 19, Rowland discloses the method of claim 18, wherein the at least one agent reports any suspicious activity that exceeds a suspicion threshold (fig. 10 controls the intrusion detection system setup and determines the suspicion thresholds).

Regarding claim 20, Rowland discloses the method of claim 19, wherein the at least one agent transmits said analyzed data in order to determine an origin of the suspicious activity in the computer network (col. 2 lines 40-67).

Regarding claim 21, Rowland discloses the method of claim 20, further comprising scanning said analyzed data for patterns and comparing said patterns to data representative of patterns of known threats to said computer network for identification of said suspicious activity (col. 5, lines 30-35 and figs. 3-4).

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aubrey H. Wyszynski whose telephone number is (571)272-8155. The examiner can normally be reached on Monday - Thursday, and alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 5712723811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

AHW